10 Network Security Steps for Every Small Business

By Sean Michael Kerner | Published on: 02-Jun-11

Back to article

Just because your business is small, doesn't mean that hackers won't target you. The reality is that automated scanning techniques and botnets don't care whether your company is big or small, they're only looking for holes in your network security to exploit.

The good news is that there are a lot of things that small businesses can do to lock down networks without spending a small fortune. Through a combination of hardware, software and best practices, you can minimize your risks and reduce the attack surface that your small business presents to the world.

10 Tips to Tighten Network Security

1. Get a Firewall

The first step for any attacker is to find network vulnerabilities by scanning for open ports. Ports are the mechanisms by which your small business network opens up and connects to the wider world of the Internet. A hacker sees an open port to as an irresistible invitation for access and exploitation. A network firewall locks down ports that don't need to be open.

A properly configured firewall acts as the first line of defense on any network. The network firewall sets the rules for which ports should be open and which ones should be closed. The only ports that should be open are ports for services that you need to run.

If you're running a Web or mail server on your network, the proper ports for those services need to be open. If you're *not* running those services directly on your own network, say for example you're hosting your website and email with a service provider, you shouldn't have your Web server and email ports open.

Typically, most small business routers include some kind of firewall functionality, so chances are if you have a router sitting behind your service provider or DSL/cable modem, you likely have a firewall already.

To check to see if you already have firewall capabilities at the router level in your network, log into your router and see if there are any settings for Firewall or Security. If you don't know how to log into your router on a Windows PC, find your Network Connection information. The item identified as **Default Gateway** is likely the IP address for your router.

There are many desktop firewall applications available today as well, but don't mistake those for a substitute for firewall that sits at the primary entry point to your small business network. You should have a firewall sitting right behind where your network connectivity comes into your business to filter out bad traffic before it can reach any desktop or any other network assets.

2. Password Protect your Firewall

Great you've got a firewall, but it's never enough to simply drop it into your network and turn it on. One of the most common mistakes in configuring network equipment is keeping the default password.

It's a trivial matter in many cases for an attacker to identify the brand and model number of a device on a network. It's equally trivial to simply use Google to obtain the user manual to find the default username and password.

Take the time to make this easy fix. Log into your router/firewall, and you'll get the option to set a password; typically you'll find it under the **Administration** menu item.

3. Update Router Firmware

Outdated router or firewall firmware is another common issue. Small business network equipment, just like applications and operating systems, needs to be updated for security and bug fixes. The firmware that your small business router and/or firewall shipped with is likely out-of-date within a year, so it's critical to make sure you update it.

Some router vendors have a simple dialogue box that lets you check for new firmware versions from within the router's administration menu. For routers that don't have automated firmware version checking, find the version number in your router admin screen, and then go to the vendor's support site to see if you have the latest version.

4. Block Pings

Most router and firewalls include multiple settings that help to determine how visible your router and/or firewall will be to the outside world. One of the simplest methods that a hacker uses to find a network is by sending a ping request, which is just a network request to see if something will respond. The idea being if a network device responds, there is something there that the hacker can then explore further and potentially exploit.

You can make it harder for attackers by simply setting your network router or firewall so that it won't respond to network pings. Typically the option to block

network pings can be found on the administration menu for a firewall and/or router as a configuration option.

5. Scan Yourself

One of the best ways to see if you have open ports or visible network vulnerabilities is to do the same thing that an attacker would do -- scan your network.

By scanning your network with the same tools that security researchers (and attackers) use, you'll see what they see. Among the most popular network scanning tools is the open source nmap tool). For Windows users, the Nmap download now includes a graphical user interface, so it's now easier than ever to scan your network with industry standard tools, for free.

Scan your network to see what ports are open (that shouldn't be), and then go back to your firewall to make the necessary changes.

6. Lock Down IP Addresses

By default, most small business routers use something called DHCP, which automatically allocates IP addresses to computers that connect to the network.

DHCP makes it easy for you to let users connect to you network, but if your network is exploited it also makes it easy for attackers to connect to your network. If your small business only has a set number of users, and you don't routinely have guest users plugging into your network, you might want to consider locking down IP addresses.

On your router/firewall admin page, there is likely a menu item under network administration that will let you specify IP addresses for DHCP users. You'll need to identify the MAC address to which you can then assign an IP (to find your MAC address read What's a MAC Address, and How Do You Find It?).

The benefit of assigning an IP is that when you check your router logs, you'll know which IP is associated with a specific PC and/or user. With DHCP, the same PC could potentially have different IPs over a period of time as machines are turned on or off. By knowing what's on your network, you'll know where problems are coming from when they do arise.

7. Use VLANs

Not everyone in your small business necessarily needs access to the same network assets. While you can determine and set access with passwords and permissions on applications, you can also segment your network with VLAN or virtual LANs.

VLANs are almost always part of any business class router and let you segment a network based on needs and risks as well as quality of service requirements. For example, with a VLAN setup you could have the finance department on one VLAN, while sales is on another. In another scenario, you could have a VLAN for your employees and then setup another one for contract or guest workers.

Mitigating risk is all about providing access to network resources to the people who are authorized and restricting access to those who aren't.

8. Get an IPS

A firewall isn't always enough to protect a small business network. Today's reality is that the bulk of all network traffic goes over Port 80 for HTTP or Web traffic. So if you leave that port open, you're still at risk from attacks that target port 80.

In addition to the firewall, Intrusion Prevention System (IPS) technology can play a key network security role. An IPS does more than simply monitor ports; it monitors the traffic flow for anomalies that could indicate malicious activity.

IPS technology can sometimes be bundled in on a router as part of a Unified Threat Management (UTM) device. Depending on the size of your small business network, you might want to consider a separate physical box.

Another option is to leverage open source technologies running on your own servers (or as virtual instances if you are virtualized). On the IPS side, one of the leading open source technologies is called SNORT (which is backed by commercial vendor Sourcefire.

9. Get a WAF

A Web Application Firewall (WAF) is specifically tasked with helping to protect against attacks that are specifically targeted against applications. If you're not hosting applications within your small business network, the risks that a WAF helps to mitigate are not as pronounced.

If you are hosting applications, WAF in front of (or as part of) your Web server is a key technology that you need to look at. Multiple vendors including Barracuda have network WAF boxes. Another option is the open source ModSecurity project, which is backed by security vendor Trustwave.

10. Use VPN

If you've gone through all the trouble of protecting your small business network, it makes sense to extend that protection to your mobile and remotely connected employees as well.

A VPN or Virtual Private Network lets your remote workers log into your network with an encrypted tunnel. That tunnel can then be used to effectively shield your remote employees with the same firewall, IPS and WAF technologies that local users benefit from.

A VPN also protects your network by not letting users who may be coming in from risky mobile environments connect in an insecure fashion.

You Can Secure Your Network

You may be a small business, but you can use these 10 tips to help secure your network. Though hackers don't discriminate against small business, they also tend to target the low-hanging fruit and the easier targets.

Lock down your network with a properly configured firewall, understand your own internal network with locked down IPs, VLANs and VPN, and you'll be ten steps ahead of the low-hanging fruit.

Small Business Computing is on Facebook. *Join us on Facebook and interact with the site's editors, post messages, share your small business challenges and successes, discuss technology and suggest topics you'd like covered on Small Business Computing.*

Do you have a comment or question about this article or other small business topics in general? Speak out in the **SmallBusinessComputing.com Forums**. Join the discussion today!